CYBER SECURITY FUNDAMENTALS
COURSE CODE: 5370

COURSE DESCRIPTION: Cyber Security Fundamentals introduces the core concepts and terminology of cyber security and information assurance. The course examines how the concept of security integrates into the importance of user involvement, security training, ethics, trust, and best practices management. The fundamental skills cover network security, testing, and validation; compliance and operational security; threats and vulnerabilities; application, data, and host security; access control and identity management; cryptography; and a broad range of other topics.

OBJECTIVE: Given the necessary equipment, supplies, and appropriate software, the student will successfully complete the standards necessary for national credentials.

COURSE CREDIT: 1 or 2 Carnegie units

PREREQUISITE: Instructor Recommendation or Networking Fundamentals or Server Administration

RECOMMENDED GRADE LEVELS: 10–12

INDUSTRY CERTIFICATION:

CompTIA Security +
http://certification.comptia.org/getCertified/certifications/security.aspx

A. SAFETY

1. Review school safety policies and procedures.
2. Review classroom safety rules and procedures.
3. Review safety procedures for using equipment in the classroom.
4. Identify major causes of work-related accidents in office environments.
5. Demonstrate safety skills in an office/work environment.

B. STUDENT ORGANIZATIONS

1. Identify the purpose and goals of a Career and Technology Student Organization (CTSO).
2. Explain how CTSOs are integral parts of specific clusters, majors, and/or courses.
3. Explain the benefits and responsibilities of being a member of a CTSO.
4. List leadership opportunities that are available to students through participation in CTSO conferences, competitions, community service, philanthropy, and other activities.
5. Explain how participation in CTSOs can promote lifelong benefits in other professional and civic organizations.

C. TECHNOLOGY KNOWLEDGE

1. Demonstrate proficiency and skills associated with the use of technologies that are common to a specific occupation.
2. Identify proper netiquette when using e-mail, social media, and other technologies for communication purposes.
3. Identify potential abuse and unethical uses of laptops, tablets, computers, and/or networks.
4. Explain the consequences of social, illegal, and unethical uses of technology (e.g., piracy; illegal downloading; licensing infringement; inappropriate uses of software, hardware, and mobile devices in the work environment).
5. Discuss legal issues and the terms of use related to copyright laws, fair use laws, and ethics pertaining to downloading of images, photographs, documents, video, sounds, music, trademarks, and other elements for personal use.
6. Describe ethical and legal practices of safeguarding the confidentiality of business-related information.
7. Describe possible threats to a laptop, tablet, computer, and/or network and methods of avoiding attacks.

D. PERSONAL QUALITIES AND EMPLOYABILITY SKILLS

1. Demonstrate punctuality.
2. Demonstrate self-representation.
3. Demonstrate work ethic.
4. Demonstrate respect.
5. Demonstrate time management.
6. Demonstrate integrity.
7. Demonstrate leadership.
8. Demonstrate teamwork and collaboration.
9. Demonstrate conflict resolution.
10. Demonstrate perseverance.
11. Demonstrate commitment.
12. Demonstrate a healthy view of competition.
13. Demonstrate a global perspective.
14. Demonstrate health and fitness.
15. Demonstrate self-direction.
16. Demonstrate lifelong learning.

E. PROFESSIONAL KNOWLEDGE

1. Demonstrate effective speaking and listening skills.
2. Demonstrate effective reading and writing skills.
3. Demonstrate mathematical reasoning.
4. Demonstrate job-specific mathematics skills.
5. Demonstrate critical-thinking and problem-solving skills.
6. Demonstrate creativity and resourcefulness.

7. Demonstrate an understanding of business ethics.
8. Demonstrate confidentiality.
9. Demonstrate an understanding of workplace structures, organizations, systems, and climates.
10. Demonstrate diversity awareness.
11. Demonstrate job acquisition and advancement skills.
12. Demonstrate task management skills.
13. Demonstrate customer-service skills.

F. INTRODUCTION TO INFORMATION ASSURANCE

1. Explain the importance of data security.
2. Explain the concepts of confidentiality, integrity, and availability (CIA).
3. Describe current events on breaches; focus on particular Information Assurance (IA) areas that were compromised.
4. Explain the importance of physical security.

G. BASIC COMPUTER AND NETWORK ARCHITECTURE

1. Build cabling (passthrough, crossover, and TAP).
2. Use a basic command line interface (Windows and Linux) to configure communications (e.g., ipconfig).
3. Design a basic network topology.

H. ADVANCED NETWORKING AND SECURITY

1. Set up Port/Network Address Translation (NAT/PAT).

I. HOST SYSTEM AND APPLICATION SECURITY

1. Compare and contrast common operating systems (e.g., Windows, Linux, OS X).
2. Compare and contrast common file systems.
3. Analyze and differentiate between types of application attacks.
4. Implement Active X and Java Security.
5. Discuss protection from buffer overflow attacks.
6. Prevent input validation attacks and scripting attacks.

J. SECURITY ADMINISTRATION

1. Analyze security using a baseline analyzer (e.g., Microsoft Baseline Security Analyzer [MBSA]).
2. Back up data using a utility (e.g., Microsoft [MS] Backup/Restore).
3. Audit Windows/Linux.
4. Select/Set file/folder permissions in Windows/Linux.
5. Set up shared documents/folders.
6. View/Edit Windows services (disable services).

7. Enable Extended File System (EFS).
8. View and change the backup archive bit.
9. Secure DNS/BIND, web, email, messaging, and FTP servers.
10. Secure directory services/DHCP/file and print servers.

K. DOMAINS SUPPORTING COMPTIA SECURITY + CERFICIATION

1.0 Network Security

1.1 Implement security configuration parameters on network devices and other technologies.
2.1 Given a scenario, use secure network administration principles.
3.1 Explain network design elements and components.
4.1 Given a scenario, implement common protocols and services.
5.1 Given a scenario, troubleshoot security issues related to wireless networking.

2.0 Compliance and Operational Security

1.1 Explain the importance of risk related concepts.
2.1 Summarize the security implications of integrating systems and data with third parties.
3.1 Given a scenario, implement appropriate risk mitigation strategies.
4.1 Given a scenario, implement basic forensic procedures.
5.1 Summarize common incident response procedures.
6.1 Explain the importance of security related awareness and training.
7.1 Compare and contrast physical security and environmental controls.
8.1 Summarize risk management best practices.
9.1 Given a scenario, select the appropriate control to meet the goals of security.

3.0 Threats and Vulnerabilities

1.1 Explain types of malware.
2.1 Summarize various types of attacks.
3.1 Summarize social engineering attacks and the associated effectiveness with each attack.
4.1 Explain types of wireless attacks.
5.1 Explain types of application attacks.
6.1 Analyze a scenario and select the appropriate type of mitigation and deterrent techniques.
7.1 Given a scenario, use appropriate tools and techniques to discover security threats and vulnerabilities.
8.1 Explain the proper use of penetration testing versus vulnerability scanning.

4.0 Application, Data, and Host Security

1.1 Explain the importance of application security controls and techniques.

2.1 Summarize mobile security concepts and technologies.

3.1 Select the appropriate solution to establish host security given a scenario.

4.1 Implement the appropriate controls to ensure data security.

5.1 Compare and contrast alternative methods to mitigate security risks in static environments.

5.0 Access Control and Identity Management

1.1 Compare and contrast the function and purpose of authentication services.

2.1 Select the appropriate authentication, authorization, or access control given a scenario.

3.1 Install and configure security controls when performing account management, based on best practices.

6.0 Cryptography

1.1 Utilize general cryptography concepts given a scenario.

2.1 Use appropriate cryptographic methods given a scenario.

3.1 Use appropriate PKI, certificate management, and associated components given a scenario.